HISPOL 008.0

The United States House of Representatives Information Security Policy for Wireless Handheld Devices

Version:	**2.0**
Approved:	**January 2010**
Approval Authority:	**The United States House of Representatives Committee on House Administration**

Table of Contents

1 Introduction

The purpose of this policy is to provide guidance for the secure operation and implementation of Internet-enabled handheld devices throughout the United States House of Representatives (House) environment. Ensuring sufficient security is a vital concern when deploying and managing wireless devices. When introducing wireless technologies into the House environment, special care and consideration must be exercised since they introduce comparable vulnerabilities as in the wired world as well as unique vulnerabilities due to their electromagnetic and portable characteristics.

1.1 Scope

This document provides the House with guidance for implementing Internet-enabled handheld devices (e.g., Personal Digital Assistant [PDA], BlackBerry, Tablet PC, or Smart Phone), whether standalone or connected as an extension of the House network. All offices that use wireless handheld devices that connect to the House network must follow this policy since the improper introduction of wireless devices in one office can create a backdoor and make not only their data and resources vulnerable but potentially put the entire House network at risk.

2 Policy Guidelines

It is essential that the following guidelines for wireless connectivity to the House network be observed to ensure the security and integrity of House-wide systems. All wireless network devices and technologies that provide a bridge between the House network and the wireless network, or any device that is designed to communicate with such a device via the wireless network, that do not comply with this policy shall not be permitted to operate. As part of the overall defense-in-depth strategy of the Information Systems Security Office (INFOSEC), both the wired and wireless networks will be monitored for unauthorized use or devices.

2.1 Authentication

Authentication is used to verify the identity of the user and provides access control to the network. The following guidelines apply:

1) All wireless device users must be authenticated to access wireless devices and/or the desktop PC synchronization software.
2) Wireless handheld devices and synchronization software must require a strong password, a token, or both to authenticate access to the device or software. Users are required to authenticate when operating locally and remotely. If voice authentication is used, password authentication must also be utilized.
3) If available, unique device identifiers should be used to authenticate the user for network access to a handheld device.

4) The "Power On" password must be enabled on handheld devices.
5) Wireless device authentication must not be disabled.
6) Timeout mechanisms that automatically prompt the user for a PIN code or password after a period of inactivity must be employed.

2.2 Encryption

1) All wireless handheld devices should encrypt information leaving the device for an adequate level of protection.
2) Wireless device default settings must not be set to "no encryption."
3) Sensitive data and application data files stored on handheld devices must be protected with robust encryption and password protection utilities. It is required that sensitive data files be deleted from the handheld device once they are no longer needed and archived on a desktop PC.
4) A virtual private network (VPN) solution should be used as a means of encrypting and authenticating the wireless traffic. If possible, all wireless communication should use strong cryptography, have robust key management, and have strong user authentication.
5) Data residing on external storage modules should be encrypted and stored in a secure manner.

2.3 Access Control

1) Data traversing wireless networks and data accessible via wireless entry must be protected from unauthorized access, use, modification, or deletion using access control methods.
2) Device lock settings must be enabled and set to lock after 30 minutes of inactivity.
3) To mitigate data leakage, Infrared (IR) ports must be disabled during periods of inactivity. The Bluetooth feature should be disabled when it's not in use. Additionally, the default password for connecting to a Bluetooth-enabled device should be changed.
4) File sharing on wireless client devices shall be disabled.
5) Only House employees and approved vendors and contractors may have access to Wireless Local Area Networks (WLANs) that connect to the House network.

2.4 Antivirus Software

All handheld devices must, whenever possible, utilize antivirus software as directed in House Information Security Policy, specifically:

1) Antivirus software for handheld devices shall scan all entry ports (i.e., beaming, synchronizing, email, and Internet downloading) as data is imported into the device, provide online signature update capabilities, and prompt the user before it deletes any suspicious files.

2.5 Personal Firewalls

Personal firewall software helps mitigate threats of confidentiality, integrity, and authenticity of information being transferred over the Internet. The following guidelines apply:

1) It is highly recommended that handheld devices utilize personal firewall software whenever possible.
2) Users that access public wireless networks (e.g., in airports, conference centers, coffee shops) should install personal firewall software on all handheld devices. A personal firewall protects against wireless network attacks and rogue access points (e.g., Ad hoc networks, accidental or malicious association, soft access points) that can be easily installed in public areas.

2.6 Physical Security

The physical security of all handheld devices is the first line of defense in WLAN security. It is essential that proper physical countermeasures be in place to mitigate risks such as theft of equipment and wireless network monitoring devices and:

1) Wireless handheld devices and Network Interface Cards (NICs) must be physically protected from loss and theft.
2) Wireless handheld devices, backup modules, and NICs (e.g., laptop computers) must be stored in a secure area, such as a desk with drawers that lock or a file cabinet that locks, when they are not being used.

2.7 Inventory, Monitoring and Audit

1) All wireless handheld devices must meet the current security configurations established byINFOSEC.
2) All wireless handheld devices may be routinely monitored and security audits performed to verify that security configurations comply with this policy, wireless devices are authorized, and to identify unauthorized activity.
3) Access logs and system audit trails shall be routinely monitored.
4) Procedures must be established and followed for the inventory and control of wireless handheld devices.

2.8 System Administration Responsibilities

1) It is the System Administrator's responsibility to ensure that wireless devices meet the technical standards outlined in this policy at all times.
2) System Administrators are required to operate wireless devices in a secure manner.
3) System Administrators are required to change factory default settings and use strong administrative passwords on all wireless devices to ensure a higher level of security. (On some wireless devices, the factory default password is blank.)
4) To the extent possible, System Administrators shall ensure that their wireless implementation and associated security technologies are up-to-date with evolving standards and best practices. Client NICs and handheld devices must support firmware upgrade so that security patches and upgrades may be fully tested and deployed as they become available.
5) System Administrators are required to maintain a list of authorized wireless device users to enable them to perform periodic inventory checks and security audits.

2.9 User Responsibilities

1) It is the wireless user's responsibility to comply with this policy.
2) Wireless users must only access information systems using approved wireless device hardware, software, solutions, and connections.
3) Wireless device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.
4) Wireless users must act appropriately to protect information, network access, passwords, cryptographic keys, and wireless equipment.
5) Wireless users are required to report any misuse, loss, or theft of wireless devices or systems immediately to INFOSEC .